# Demonstrate an awareness of ethics and professionalism for the computer industry in South Africa 114055

This unit standard is intended:

To provide conceptual knowledge of the areas covered

For those working in, or entering the workplace in the area of Information Technology

As additional knowledge for those wanting to understand the areas covered

People credited with this unit standard are able to:

Describe professionalism for the computer industry in South Africa

Describe the codes of practice for professionalism in the IT industry in South Africa

Describe the code of ethics in the computer industry in South Africa

The performance of all elements is to a standard that allows for further learning in this area.

LEARNING ASSUMED TO BE IN PLACE AND RECOGNITION OF PRIOR LEARNING

The credit value of this unit is based on a person having prior knowledge and skills to:

Describe the management and use of computers in organisations

# INDEX

# Unit Standard 114055 – Alignment Index

| SPECIFIC OUTCOMES AND RELATED ASSESSMENT CRITERIA | | Page |
|---|---|---|
| **SO 1** | **Describe professionalism for the computer industry in South Africa** | |
| AC 1 | The description identifies acceptable and unacceptable professional practices found in the computer industry. | |
| AC 2 | The description identifies known professional bodies in South Africa. Range: Includes but is not limited to: CSSA; BITF; ITUC; ITA (at least 2) | |
| AC 3 | A short description of each named professional body is provided | |
| **SO 2** | **Describe the codes of practice for professionalism in the IT industry in South Africa** | |
| AC 1 | The description identifies the codes of practice for the IT industry in South Africa. | |
| AC 2 | The description provides a brief explanation of the codes of practice identified | |
| **SO 3** | **Describe the code of ethics in the computer industry in South Africa** | |
| AC 1 | The description confirms that the computer industry supports equality of opportunity. | |
| AC 2 | The description confirms the understanding that the computer industry is against computer software piracy | |
| AC 3 | The description identifies ways in which piracy is addressed in South Africa | |

## CRITICAL CROSS FIELD OUTCOMES

UNIT STANDARD CCFO ORGANISING
Organise and manage him/her self and his/her activities responsibly and effectively.

UNIT STANDARD CCFO COLLECTING
Collect, analyse, organise, and critically evaluate information.

UNIT STANDARD CCFO DEMONSTRATING
Demonstrate an understanding of the world as a set of related systems by recognising that problem solving contexts do not exists in isolation.

UNIT STANDARD CCFO CONTRIBUTING
Contribute to his/her full personal development and the social and economic development of the society at large by being aware of the importance of: reflecting on and exploring a variety of strategies to learn more effectively, exploring education and career opportunities and developing entrepreneurial opportunities

## ESSENTIAL EMBEDDED KNOWLEDGE

1. Performance of all elements is to be carried out in accordance with organisation standards and procedures, unless otherwise stated. Organisation standards and procedures may cover: quality assurance, documentation, security, communication, health and safety, and personal behaviour. An example of the standards expected is the standards found in ISO 9000 Certified Organisations.

2. Performance of all elements complies with the laws of South Africa, especially with regard to copyright, privacy, health and safety, and consumer rights.

3. All activities must comply with any policies, procedures and requirements of the organisations involved, the ethical codes of relevant professional bodies and any relevant legislative and/ or regulatory requirements.

**SOUTH AFRICAN QUALIFICATIONS AUTHORITY**

**REGISTERED UNIT STANDARD:**

## Demonstrate an awareness of ethics and professionalism for the computer industry in South Africa

| | | | | |
|---|---|---|---|---|
| **SAQA ID** | **UNIT STANDARD TITLE** | | | |
| 114055 | Demonstrate an awareness of ethics and professionalism for the computer industry in South Africa | | | |
| **ORIGINATOR** | | | | |
| SGB Information Systems and Technology | | | | |
| **FIELD** | | | **SUBFIELD** | |
| Field 10 - Physical, Mathematical, Computer and Life Sciences | | | Information Technology and Computer Sciences | |
| **ABET BAND** | **UNIT STANDARD TYPE** | **PRE-2009 NQF LEVEL** | **NQF LEVEL** | **CREDITS** |
| Undefined | Regular | Level 5 | Level TBA: Pre-2009 was L5 | 3 |
| **REGISTRATION STATUS** | | **REGISTRATION START DATE** | **REGISTRATION END DATE** | **SAQA DECISION NUMBER** |
| Reregistered | | 2018-07-01 | 2023-06-30 | SAQA 06120/18 |
| **LAST DATE FOR ENROLMENT** | | **LAST DATE FOR ACHIEVEMENT** | | |
| 2024-06-30 | | 2027-06-30 | | |

*In all of the tables in this document, both the pre-2009 NQF Level and the NQF Level is shown. In the text (purpose statements, qualification rules, etc), any references to NQF Levels are to the pre-2009 levels unless specifically stated otherwise.*

This unit standard does not replace any other unit standard and is not replaced by any other unit standard.

### PURPOSE OF THE UNIT STANDARD

This unit standard is intended:

- To provide conceptual knowledge of the areas covered
- For those working in, or entering the workplace in the area of Information Technology
- As additional knowledge for those wanting to understand the areas covered

People credited with this unit standard are able to:

- Describe professionalism for the computer industry in South Africa
- Describe the codes of practice for professionalism in the IT industry in South Africa
- Describe the code of ethics in the computer industry in South Africa

The performance of all elements is to a standard that allows for further learning in this area.

### LEARNING ASSUMED TO BE IN PLACE AND RECOGNITION OF PRIOR LEARNING

The credit value of this unit is based on a person having prior knowledge and skills to:

- Describe the management and use of computers in organisations

### UNIT STANDARD RANGE

N/A

# Specific Outcomes and Assessment Criteria:

**SPECIFIC OUTCOME 1**

Describe professionalism for the computer industry in South Africa.

**ASSESSMENT CRITERIA**

**ASSESSMENT CRITERION 1**

1. The description identifies acceptable and unacceptable professional practices found in the computer industry.

**ASSESSMENT CRITERION 2**

2. The description identifies known professional bodies in South Africa.

**ASSESSMENT CRITERION RANGE**

Includes but is not limited to: CSSA; BITF; ITUC; ITA (at least 2)

**ASSESSMENT CRITERION 3**

3. A short description of each named professional body is provided.

**ASSESSMENT CRITERION RANGE**

As for criteria 1.2

**SPECIFIC OUTCOME 2**

Describe the codes of practice for professionalism in the IT industry in South Africa.

**ASSESSMENT CRITERIA**

**ASSESSMENT CRITERION 1**

1. The description identifies the codes of practice for the IT industry in South Africa.

**ASSESSMENT CRITERION 2**

2. The description provides a brief explanation of the codes of practice identified.

**SPECIFIC OUTCOME 3**

Describe the code of ethics in the computer industry in South Africa.

**ASSESSMENT CRITERIA**

**ASSESSMENT CRITERION 1**

1. The description confirms that the computer industry supports equality of opportunity.

**ASSESSMENT CRITERION 2**

2. The description confirms the understanding that the computer industry is against computer software piracy.

**ASSESSMENT CRITERION 3**

3. The description identifies ways in which piracy is addressed in South Africa.

### UNIT STANDARD ACCREDITATION AND MODERATION OPTIONS

The relevant Education and Training Quality Authority (ETQA) must accredit providers before they can offer programs of education and training assessed against unit standards.

Moderation Process:
Moderation of assessment will be overseen by the relevant ETQA according to the moderation guidelines in the relevant qualification and the agreed ETQA procedures.

### UNIT STANDARD ESSENTIAL EMBEDDED KNOWLEDGE

1. Performance of all elements is to be carried out in accordance with organisation standards and procedures, unless otherwise stated. Organisation standards and procedures may cover: quality assurance, documentation, security, communication, health and safety, and personal behaviour. An example of the standards expected is the standards found in ISO 9000 Certified Organisations.

2. Performance of all elements complies with the laws of South Africa, especially with regard to copyright, privacy, health and safety, and consumer rights.

3. All activities must comply with any policies, procedures and requirements of the organisations involved, the ethical codes of relevant professional bodies and any relevant legislative and/ or regulatory requirements.

## Critical Cross-field Outcomes (CCFO):

### UNIT STANDARD CCFO ORGANISING

Organise and manage him/her self and his/her activities responsibly and effectively.

### UNIT STANDARD CCFO COLLECTING

Collect, analyse, organise, and critically evaluate information.

### UNIT STANDARD CCFO DEMONSTRATING

Demonstrate an understanding of the world as a set of related systems by recognising that problem solving contexts do not exists in isolation.

### UNIT STANDARD CCFO CONTRIBUTING

Contribute to his/her full personal development and the social and economic development of the society at large by being aware of the importance of: reflecting on and exploring a variety of strategies to learn more effectively, exploring education and career opportunities and developing entrepreneurial opportunities.

### REREGISTRATION HISTORY

As per the SAQA Board decision/s at that time, this unit standard was Reregistered in 2012; 2015.

### UNIT STANDARD NOTES

Works effectively with others by working co-operatively to achieve a security goals.

Supplementary information:
1. Assessment may be made on the basis of evidence of demonstrated performance in actual or simulated work situations that encompass the scope of this unit standard. This will allow the use of various approaches to assessment and presentation of evidence.
2. Consistency of performance in a range of situations must be demonstrated, albeit within particular organisational contexts, together with the knowledge and understanding of underlying concepts and principles needed for competent performance of the elements and performance criteria.
Sub-Sub-Field (Domain):
Information Systems and Technology Management

# Professionalism and Codes of Practice for the computer industry in South Africa

Time: 180 minutes Activity: Self and

The Constitution is an important tool for the Information Society, guiding the way we operate. At the AGM on the 22nd July 2004, this amended version of the Constitution was adopted. The previous version was registered in terms of the Companies Act in 1970, so has been updated to reflect today's environment.

**The Constitution**

[Registered in terms of Section 21 of the Companies Act, Act No. 46/1926 as amended and remains incorporated not for gain in terms of Section 21 of the Companies Act No. 61/1973 as amended]. The Society is established to elevate Information and Communications Technology [ICT] capability and professionalism in South Africa, specifically:

- To facilitate the exchange of opinions and views on Information and Communications Technology ICT, and to inform and promote knowledge of ICT to members and the public for the development and use of ICT
- By representing industry practitioners, to inform and lobby Government on ICT policy
- To obtain from members and other sources information relating to ICT, and to disseminate such information amongst the public and the Society by means of journals, circulars, publications, lectures, seminars, conferences or otherwise \
- To improve the technical and general knowledge and to elevate the professional status, of persons engaged in ICT.
- Education and training to elevate the level of ICT capability in South Africa.
- Professional development and advancement.
- Community development that enhances the standards and levels of ICT for the greater good of the South African people.
- To do all such other lawful things as are incidental or conducive to the attainment of the above purposes.

The following is the generally accepted Codes of Good Practice in the South African IT industry, as set out by the Computer Society of South Africa, one of, if not the most respected associations concerned with the South African Information Technology.

This Code of Practice is directed to all professional members of the Computer Society of South Africa [CSSA]. It consists, essentially, of a series of statements that prescribe minimum standards of practice, to be observed by members.

The Code is concerned with professional responsibility. All members have responsibilities – to clients, to users, to the State and to society at large. Those members who are employees also have responsibilities to their employers and employers' customers and, often, to a Trade Union. In the event of an apparent clash in responsibilities, obligations or prescribed practice the Society should be consulted at the earliest opportunity.

The Code is to be viewed as a whole: Individual parts are not intended to be used in isolation to justify errors of omission or commission. The Code is intended to be observed in the spirit and not merely to the word.

The CSSA membership covers all occupations relevant to the use of computers and it is not possible to define the Code in terms directly relevant to each individual member. For this reason the Code is set out in two levels to enable every member to reach appropriate interpretations.

**Foreword**

Any code may be considered as a formalisation of experience into a set of rules. A code is adopted by a community because its members accept that adherence to such rules, including the restrictions this implies, is of benefit to all, inside and outside the community alike. A code also has an educational role, by setting out what is required of those wishing to join the community.

It may be said that everything contained in an acceptable code is obvious and merely common sense. This, however, does not lessen its worth. The conscious selection and emphasis of a group of "common sense" items on the basis of experience is by itself a worthwhile exercise.

The Code of Practice deals with the ways in which all members of the Society are expected to exercise their professional competence and thereby complements its companion, the Code of Conduct, which deals with behaviour. The two codes apply to all professional members of the Society.

Because they are the distillation of considerable experience they set standard for all engaged in the computing profession. At a time when computing is playing an ever increasing part in national life, whether in business, industry or social affairs, it is important for the profession to state clearly what its rules are.

**Introduction**

This Code of Practice is directed to all professional members of the Computer Society of South Africa [CSSA]. It consists, essentially, of a series of statements that prescribe minimum standards of practice, to be observed by members.

The Code is concerned with professional responsibility. All members have responsibilities – to clients, to users, to the State and to society at large. Those members who are employees also have responsibilities to their employers and employers' customers and, often, to a Trade Union. In the event of an apparent clash in responsibilities, obligations or prescribed practice the Society should be consulted at the earliest opportunity.

The Code is to be viewed as a whole: Individual parts are not intended to be used in isolation to justify errors of omission or commission.

The Code is intended to be observed in the spirit and not merely to the word. The CSSA membership covers all occupations relevant to the use of computers and it is not possible to define the Code in terms directly relevant to each individual member. For this reason the Code is set out in two levels to enable every member to reach appropriate interpretations.

**Level One**

A series of brief statements defining the elements of practice to be observed

**Level Two**

The rationale for the Level One statements
Level Two is not intended as guidance on how to carry out the Code of Practice, but only to provide an explanation of its meaning and the reason for including the statement at Level One.

Where examples are given on how to apply the Code, these are simply to clarify the meaning. Many of the clauses may seem to state the obvious, but much that goes wrong in computer use does so because the obvious has been overlooked.

**Terminology**

The following conventions apply to the reading of this Code.

1. “A member” includes all categories of corporate membership defined in the Society’s Articles of Association.

2. “Client” is any person, department or organisation for whom the member works, or undertakes to provide computer-based aid, in any way.

3. “User” is any person, department or organisation served by computer based systems.

4. “System” means all applications involving the use of computer and information technology. The term does not imply any particular mode of processing, eg local batch or remote real time, etc. “System” may be interpreted as encompassing non-computer procedures and disciplines, eg clerical, manual, etc.

**Layout**

Level One appears on the left, Level Two on the right, the rationale being opposite the appropriate statement.

In one appears of their profession members will, to the extent that they are responsible:

1.1 Keep themselves, and subordinates, informed of new technologies, practices, legal requirements and standards as are relevant to their duties.

1.1 Others will expect you to provide special skills and advice and, in order to do so, you must keep yourself up-to-date. This is true for members of all professions, but particularly so in computing which is developing and changing rapidly. You must also encourage your staff and colleagues to do the same, as it is impossible to retain your professional standing by relying only on the state of your knowledge and competence at the time you achieved professional status.

1.2 Ensure subordinates are trained on an equal opportunity basis, in order to be effective in their duties and to qualify for increased responsibilities.

1.2 You should regularly review the training needs of your staff and take action to ensure that your hard-won knowledge and experience is passed on in such a way that those who receive it not only improve their own effectiveness in their present positions but also become keen to advance their careers and take on additional responsibilities.

1.3 Accept only such work as they believe they are competent to perform and not hesitate to obtain additional expertise from appropriate qualified individuals where advisable.

1.3 You should always be aware of your own limitations and not knowingly imply that you have competence you do not possess. This is of course distinct from accepting a task the successful completion of which requires expertise additional to your own. This point is central to the CSSA Code of Conduct; you cannot possibly be knowledgeable on all facts but you should be able to recognise when you need additional expertise and information and where to find it.

1.4 Actively seek opportunities for increasing efficiency and effectiveness to the benefit of the user and of the ultimate recipient.

1.4 Whatever the precise terms of your brief, you should always be aware of the environment surrounding it and not work solely towards completion of the defined task and no more. You must regard it as part of your duty to make your client aware of other needs that emerge, unsatisfactory procedures that need modification and benefits that might be achieved. You, as an innovator, should take into account the relevance of new methods and should always be looking for possibility of additional benefits not foreseen when the project was planned. You must also look beyond the immediate requirements to the needs of the ultimate user. For example, the Invoice your system produces may be right for company accounting procedures but confusing for the person who is being expected to pay against it

**2. Organisation and Management**

[This section of the Code is concerned with broad principles. Management of development is covered in detail in Sections 5 and 6; management of operational projects in Section 7. Since computer management is still management, the normal principles applicable to any kind of management apply here also].

2.1 Plan, establish and review objectives, tasks and organisational structures for themselves and subordinates, to help meet overall objectives.

2.1 It is dangerously easy for you as a computer professional to become fully engrossed in the problem of the moment, and to lose sight of the overall objectives of the organisation. Computing no less than any other discipline is an organic component of the organisation, and you should continuously ensure that the path you are following is in line with the objectives of that organisation. You must make use of the well established management practices of monitoring and review to ensure the area of work for which you are responsible is making its maximum contribution.

2.2 Ensure that any specific tasks are assigned to individuals according to their known ability and competence.

2.2 When delegating work to your subordinates, ensure that as far as possible the task will develop their competence and increase their motivation. However, you must also ensure that the principles implied in 1.3 are observed or you will be faced with unsatisfied users who are not receiving the service to which they are entitled.

2.3 Establish and maintain channels of communication from and to seniors, equals and subordinates.

2.3 It is often assumed that communication will look after itself, but good communication is vital to business success. You must ensure that formal channels of communication exist upwards, downwards and sideways in the organisation for which you are responsible. It is difficult to over emphasise this point in connection with computer work which by nature requires constant interaction between the members of the computer organisation and, most importantly, with the users. Furthermore, you will find that communication skills can be improved considerably by formal training, and this should be included in your training plans as a high priority item.

2.4 Be accountable for the quality, timeliness and use of resources in the work for which they are responsible.

2.4 High on your list of professional duties will be the requirement to provide a service of agreed quality, on time and within budget. Beyond that, of course, is the requirement for contingency planning and the need to make others affected aware of difficulties and dangers if these are foreseeable. For this you, as a professional, are responsible. You cannot turn your back on a problem once encountered, and hope someone else will solve it or that it will simply go away. Action taken to minimise the impact of such problems will, in the end, ensure a smoother running organisation.

### 3. Contracting

[This section is included in the Code because some formal agreement - even if not a specific contract - is needed before any project is started. Commitment and definition of responsibilities are essential, in advance of action].

3.1 Seek expert advice in the preparation of any formal contract.

3.1 In the same way as you would expect to be consulted in your field as a computer professional, be ready to consult other specialists when you need guidance in drawing up contracts or in matters such as commerce, finance, tax, law or risk evaluation. Much of your time can be saved in this way, to say nothing of avoiding the potential dangers of a badly drawn up contract or wrong assessment of a legal situation. Many of these areas have become defined as standard practice and a number of professional bodies provide "standard contract" forms as a guide to their own members, which helps considerably to reduce problem areas.

3.2 Ensure that all requirements and the practical responsibilities of all parties are adequately covered in any contract or tendering procedures.

3.2 In the same way as you would carefully review the completeness of the detail for a system specification, it is necessary to review the totality of the detail to be covered by a contract. Take care to ensure that such items as provision of accommodation, typing, data preparation, responsibility for media security and standby arrangements are not forgotten.

Apart from the problems which will arise if these things have been overlooked, the profitability of your contract will be adversely affected. Again, communication enters into this as you need to ensure that everyone who is party to the contract is fully aware of his obligations.

**4. Privacy, Security and Integrity**

[A system is at risk from the moment that the project that develops it is first conceived. This risk remains at least until after the system is finally discontinued, perhaps indefinitely. Threats to security range from incompetence, accident and carelessness to deliberate theft, fraud, espionage or malicious attack].

4.1 Ascertain and evaluate all potential risks in a particular project with regard to the cost, effectiveness and practicality of proposed levels of security.

4.1 One of your more difficult responsibilities is that of determining the value of a system in terms of what would be lost if security was to be breached [eg. damage to national security by leaks of military data, personal privacy by leaks from medical records or fraud by access to financial information]. However, a view is required to aid decision making, covering how much should be spent on system security in at least these four areas:

- Protection - preventing threats from becoming reality.
- Detection - in time to take suppressive action.
- Suppression - to limit the effect.
- Recovery - to rectify and get the system going.

4.2 Recommend appropriate levels of security, commensurate with the anticipated risks, and appropriate to the needs of the client.

4.2 You still need to remember that you must give attention to some areas of risk which are mandatory such as those covered by legislation for health and safety at work. However, risks exist in connection with the security and people, all of which should be identified and recommendations made.

4.3 Apply, monitor and report upon the effectiveness of the agreed levels of security.

4.3 Situations are always changing and people are liable to become lax in observing routine practices. You will therefore find an on-going security audit extremely valuable in keeping people aware of security requirements and procedures, and in the identification of weaknesses and loopholes in the security system. Moreover, security arrangements should be reviewed periodically in light of developing technology and the new methods of breaching security.

4.4 Ensure that all staff are trained to take effective action to protect life, data and equipment [in that order] in the event of disaster.

4.4 Naturally, the safety of people is your first priority, and the proper backup facilities for recreation of data files should exist. Equipment should be replaceable and normally insured. Your staff should be trained to react with regard to these priorities. Damaging a data processing centre will usually result in serious consequential losses to the business of the organisations involved. As a professional, you will be concerned to treat security drills as a serious matter and to carry it out regularly along with training all involved to be on the lookout for anything unusual.

4.5 Take all reasonable measures to protect confidential information from inadvertent or deliberate improper access or use.

4.5 Your responsibility for confidentiality of information is at least as great as that of members of other professions. The job is even more complex by reason of the speed, capacity and facility for data exchange by computers. Frequently, personal information will be under your control, and you should always be aware of the spirit and letter of relevant legislation and guidelines written to protect the individual.

4.6 Ensure that competent people are assigned to be responsible for the accuracy and integrity of the data in the data files and each part of an organisation's database.

4.6 You must take direct action to give responsibility to specific individuals to ensure the accuracy and integrity of data within each system. Whilst this is important for any system, however simple, it becomes even more significant in more complex databases and communications environments.

4.7 Ensure that, where data is stored which may be dangerous to an individual, the individual concerned has adequate rights of review, correction and appeal

4.7 Computer databases often contain information which can seriously impact the freedom of action of private individuals. A frequent example is the storage of credit information. Situations will occasionally arise where this information is incorrect, or where it may be subject to different viewpoints, such as where an account is unpaid because of a legitimate dispute. In these situations, procedures should be developed to allow the affected person to review the information held in the database and, if such person believes it to be incorrect, to have it rectified or at least to have his viewpoint incorporated. This protection becomes even more important when data obtained for one purpose [or by one organisation] is used for another purpose [or by other organisations].

**5. Development**

["Development" in this context means not only all the work involved in order to reach the stage where a viable computer system is ready to become operational; it also includes all the activities involved in installing the system in its eventual production environment].

5.1 Exercise impartiality when evaluating each project with respect to its technical, moral and economic benefits.

5.1 Your responsibility in a project will give you opportunities to make decisions based on your personal views and preferences. The line between personal bias and professional opinion becomes somewhat finely drawn. To avoid finding yourself on the wrong side of the line, always make sure you are aware of your client's objectives and the benefits he/she is looking for, and be careful not to lose objectivity through enthusiasm created by the latest technological developments.

5.2 Effectively plan, monitor, adjust and report on all development, acquisition or replacement projects.

5.2 This principle is no different from that applying to many other fields, but your attention is drawn to it at it is essential to business control in any organisation.

5.3 Ensure that effective standard procedures and documentation are available and used.

5.3 A characteristic of professionals is that they depend on the operation of a series of standards and procedures for efficiency and professional results. You should ensure that the standards you lay down do not cause inhibiting rigidity, but provide a framework within which individuals know how, when and by whom the work is to be done.

5.4 Specify the system objectives, completion date, cost and security requirements for the client and the necessary criteria for their achievement.

5.4 Always ensure that you produce a clear statement with qualified objectives wherever possible which can be agreed to with the client. It is all too easy to overlook this point in the general rush of business life: when committing agreements to paper it is frequently a neglected activity. For large projects covering a significant span of time, objectives should in fact be regularly reviewed to ensure that the project is still relevant in the light of changing circumstances.

5.5 Ensure that the client can participate in all stages of problem analysis, system development and implementation.

5.5 The system you develop ultimately belong to your client, and therefore he/she needs to maintain control and be given opportunities to exercise them. Therefore you should seek his/her involvement in key project activities, e.g. the specification, quality control and provision of test data. You should encourage and help the client to achieve the right level of involvement not less because in this way you ensure that you produce the system that the client requires.

5.6 Ensure that each task is completed to a defined level before the next dependent task is started.

5.6 A task may be anything from specifying a system to determining the size of a piece of detailed code. While many tasks will be executed in parallel, dependent tasks should be completed sequentially with nondependent activities within them overlapped. Should you not, for example, start writing a program in advance of a complete specification if you wish to avoid duplication or loss of effort.

5.7 Specify and conduct program tests and system tests to ensure that all system objectives are met to satisfaction of the client.

5.7 It is clearly necessary for you to test each program separately and then all programs together as a complete suite, followed by the computer elements together with the rest of the system. The objective is to prove the system functions as intended and not merely to detect errors. The client should be involved in the testing to achieve the objectives in 5.5.

5.8 Ensure that systems are designed and sufficiently documented to facilitate subsequent audit, maintenance and enhancement, and accurate comprehension by users.

5.8 It is essential, at the originating stage that you consider and provide for the needs of future audit and modification. Documentation should also assist troubleshooting and enable modification to be undertaken with minimal reprogramming and the smallest possible impact on operations. Also your users will require documentation in a convenient form to enable them to understand and properly utilise the system.

5.9 Ensure that input and output are designed to obviate misunderstanding.

5.9 The input and output of a system is normally prepared or received by non-technical users and consequently must be designed to simplify business life rather than add extra burdens. Input and output should be easily readable - avoid jargon, unfamiliar codes and abbreviations - and provide clear headings and such things as page numbers. Whenever possible, the power of the computer should be used so as permit the maximum use of plain language.

5.10 Ensure that there are adequate procedures available to delete erroneous, redundant and out of date data from files.

5.10 It is part of a sound approach to consider not only the immediate use of a system but also its effectiveness during a life which will be as long as it continues to meet its objectives. During this life, redundant data is bound to accumulate and it will be essential to periodically remove such data. Also due, to system weaknesses and clerical procedures, undisciplined corrections or deletions may occur, thereby compounding the problem, and possibly resulting in the system producing erroneous results.

5.11 Ensure that adequate procedures are available which will, with the minimum of inconvenience, restore data files and program files to their required conditions in the event of data loss, corruption or system failure.

5.11 This is complementary to 4.1. The design stage is the time to ensure that the restorative procedures are incorporated. When an operational disaster occurs it will be too late to start thinking about such procedures. The emphasis in 5.10 and 5.11 is on clear procedures to protect data and programs from corruption rather than relying on ad hoc correction by individuals who may subsequently be the only ones who know what they have done.

5.12 Ensure that projects are completed with technical soundness, using the most appropriate technology and within time and cost constraints.

5.12 Cost and service are criteria of an effective system rather than technical ingenuity. The technology to be exploited should be the best for the client's problem not necessarily the most sophisticated.

### 6. Implementation

[The term is used here to describe the transition form development to full operation].

6.1 Ensure that adequate provision is made for user and operations staff training in all functions of the system for which they are responsible.

6.1 You should not consider the task complete until you have seen the new system through to implementation. Your professional duty requires you to see that the system can be used effectively by your client's staff.

Each new system will bring with it, to some degree, new approaches, new techniques and new ways of doing things. These have to be explained to your users who may show resistance to change because of their previous experience. You should recognise that they will require time to become familiar with the new system and to gain confidence and ability to meet the new conditions. Training in advance of implementation is normally essential to countering these problems.

6.2 Effectively plan, monitor, adjust and report upon all activities concerned with the changeover from development to operational running.

6.2 These are vital parts of the design and development process. Your plans should specify in detail all resources involved whether user's or computer staff. Further constant reviewing will be necessary as implementation responsibilities will be put to the test here, as all who are affected will need to be advised of changes and be given the opportunity to comment. Again the opportunity presents itself to help generate the understanding, confidence and sense of involvement so necessary to successful implementation and subsequent operation. If you fail to carry out these functions effectively, operation dates will be jeopardised and, almost certainly, implementation costs will be higher than they need be.

6.3 Ensure expeditious and economic completion of implementation consistent with adequate testing and security.
6.3 Here you are involved in a professional judgement or trade-off between under and over testing. If you cut corners by, say, reducing system testing time, then the likely effect on the operation elsewhere should be evaluated and made known to those who should know.

**7. Live Systems**

[This section is concerned with the ongoing operation of systems handed over by design and development staff].
7.1 Plan and operate efficient and reliable processing within defined budgets.
7.1 "Processing services" covers all the activities between reception of data and delivery of results. You must ensure that these services are provided efficiently to users who are just as dependent on these as they are on the application software for the well being of their business.
7.2 Monitor performance and quality and arrange regular reviews of the efficiency, effectiveness and security of live systems.
7.2 The dynamic nature of most business environments means that, over a period, a system may gradually provide the user with a system of reduced value and quality. Regular post-implementation reviews will be all the more effective if you check not only how well the system is meeting its original objectives, but also how it has evolved in the light of current business requirements.
7.3 Plan, from the start of a project, to provide adequate maintenance and enhancement support to live systems so that they continue to meet all requirements.
7.3 Much of the criticism computer applications receive is traceable to their failure to respond, by means of modification, to changing conditions. Either modifications do not happen, or they implemented haphazardly over too long a period. If you ensure that your project plans include provision of a formal system to control the enhancement of programs, and identify the need for appropriate maintenance resources, you will avoid user dissatisfaction arising from this type of problem.
7.4 Establish good liaison with users and provide proper facilities for dealing with enquiries and day-to-day problems concerning the user of their systems.
7.4 One of the most important areas where your professional skill will be required is in maintaining continuous formal and informal liaison with your users. All those concerned with the services which you are responsible for providing should know and understand the need for formal channels of communication. In particular, do not forget to ensure that these exist to cover the special circumstances which arise in emergencies.

## Professional Computer Bodies in South Africa

***CSSA*** – The above section is directly derived from the CSSA

***BITF*** - The Black Information Technology Forum (BITF) was launched in Cape Town in 1995 to propel black individuals into the mainstream of the Information and Communication Technology (ICT) industry.

A Gauteng branch was formed in 1997 and the forum became a national organisation in 1998. Currently there are branches in Gauteng, KwaZulu Natal, Western Cape, Limpopo, Eastern Cape and Mpulamlanga serving the interests of 2 400 members.

Efforts are being made to establish branches in Northern Cape and North West Province. It is the largest organisation representing the interests of black people in South Africa's ICT industry and has considerable credibility with government bodies.

The BITF aims to:

- Empower members with technical and business skills;
- Make BITF members significant role players within the ICT sector;
- Improve access to technology for historically disadvantaged communities;
- Actively influence policy -making forums, and
- Promote the status of historically disadvantaged individuals and communities in the ICT sector.

BITF focuses on two programmes:

- One which seeks to facilitate the development of skills throughout the technology sector and foster internships and experiential training by engaging corporate South Africa and multinationals, and
- The ABC Programme that promotes governance and provides a framework that guides the implementation of black economic empowerment.

***ITUC*** - The **International Trade Union Confederation** (ITUC) is the world's largest trade union federation. It was formed on 1 November 2006 out of the merger of the International Confederation of Free Trade Unions (ICFTU) and the World Confederation of Labour (WCL). This union assists the South African IT market in trading internationally, thus empowering the market, but more-so those in the emerging sector of the market.

***ITA -*** The ITA stands at the threshold of a new era for the local Information, Communication and Technology (ICT) Sector. The representative body, together with its membership and industry partners, is poised to play a crucial role in the growth and development of the sector, as well as serving as a credible, effective channel of communication between various stakeholders. The purpose of the ITA as stated in its Constitution is to "***represent and promote the interests of its members, which shall be employers active in the Information Technology Sector***."

Furthermore, the ITA is defined as:

- A body of members actively participating in issues and events, which directly or indirectly affect business.
- The members initiate issues, which need attention at international and national governmental, NGO, parastatal and business level.

***History of the ITA***

The ITA was founded in 1934 and was officially renamed the Information Technology Association (ITA) after the amalgamation of the Business Equipment Association (BEA) and the Computer Services Association.

The ITA is the official trade and employer body of the ICTe Industry and strives to promote consistent standards of professionalism and service in the ICTe Industry.

| | |
|---|---|
| 1934: | Transvaal Typewriter and Office Appliance Traders Association |
| 1938: | Typewriter and Office Appliance Association of South Africa |
| 1956: | Office Appliances Association of South Africa |
| 1967: | Business Equipment Association of South Africa |
| 1989: | BEA ITA of South Africa |
| 1996: | Information Technology Association of South Africa |

### ***Primary Business of the ITA***

To promote and represent collectively the ICTe Industry, nationally and internationally at governmental, NGO, parastatal and business level.

- To assemble and disseminate information and communicate such with the membership base.
- To provide a networking and marketing platform for the membership base.
- To encourage the formation of interest groups who can collectively influence and be party to the setting of standards and strategies for the ICTe industry, as well as legislation affecting the industry at large.

### ***Divisions of the ITA***

The ITA operates through and Executive Council and three specialist sector divisions including:

- **The Information Technology Users Council (ITUC)**. The ITUC's main function is to provide and effective facility through which training providers, students, prospective employers and institutions can guarantee the authenticity and credibility of the Cobalt examination process.
- **Recruitment Consultancy Services Group (ITARCS)**. ITARCS has been set up to address recruitment and contracting issues within the IT Industry with reference to the Labour Relations Act and other employment legislation.
- **Payroll Authors Group (PAG)**. The PAG aims to liaise with government departments and statutory bodies to maintain awareness of legislative changes and ensure that payroll software incorporates legislative changes.

**Activity – Questioning – In your groups**

Identify and explain acceptable and unacceptable professional practices found in the computer industry

Identify and explain each of the following professional bodies in South Africa.

CSSA

BITF

ITUC

ITA

Identify and explain the codes of practice for the IT industry in South Africa

## Code of ethics in the computer industry in South Africa

Time: 90 minutes Activity: Self and Group

**What is Piracy?**

Software piracy has become an important topic affecting the software industry internationally, including individual and business users of all software products worldwide.

Software piracy is the failure to comply with software license agreements. Piracy, in any form, is an unlawful action and offenders are liable to either civil or criminal prosecution. It is important that all software users and resellers understand the different forms of software piracy in order to comply with the law and protect themselves and their business.

**The various forms of software piracy are:**

- End User Copying - A licensed software user passes their software onto friends, business colleagues and family to copy indiscriminately. Or in the case of volume software licenses, users and/or businesses under report the number of computers in which the software is installed.
- Reseller Copying - Resellers pass their software onto their clients.
- Counterfeiting - Criminals copy the software and collateral, such as manuals, and sell it as the original product.

Software piracy negatively impacts customers, resellers and software vendors. Lower vendor revenues, as a result of software piracy, limit the industry's ability to re-invest funds in research and development (R&D) and continuously maintain and improve service and support infrastructures. Ongoing investment in R&D ensures that software vendors have the ability to keep their users at the forefront of the latest technology developments.

Furthermore, purchasing pirate software can have a damaging effect on your company as the software may introduce viruses to your system, destroying mission critical data. Users of pirate products do not benefit from the quality and reliability guarantees provided to lawful, licensed customers and will be unable to access technical software support.

**Let’s look at an example of piracy in today’s industry:**

**Music Piracy**

***Q: A few weeks ago a friend 'burned' me a pirate copy of a new CD he'd just bought. It's not a band I would usually have bothered with, but I have to admit the music is pretty good. However I now feel guilty every time I play the CD. Should I give the CD back, and risk alienating my friend? Should I just throw it away and hope he doesn't raise it in conversation, forcing me into an awkward situation? Or can I keep the CD with a clear conscience, knowing that I didn't make the illegal copy, and that it's pretty unlikely that I would ever have bought a copy anyway?***

*A: Music piracy, while not as sexy as the old skull-and-crossbones kind, is certainly a good deal more widespread. 'Piracy' is generally considered to include a) 'pirate recordings', where it's just the music itself that is copied, usually by ordinary people using ordinary equipment on a not-for-profit basis ('Dude, I just got the new Kaiser Chiefs album - do you want me to burn you a copy?'); b) 'counterfeiting', which involves copying the music as well as the packaging, and generally involves attempting to pass off the copy as the real thing; c) 'online piracy', which is basically the same as either making a pirate recording or counterfeiting, only it's done via the internet; and d) 'bootlegging', which is the recording and trading of a performance, usually a live concert, which has not been officially released by the artist or her representative.*

*RIAA, the Recording Industry Association of America, claims that the recording industry 'loses' around 4.2 billion U.S. dollars to piracy each year. This figure is reached by way of an inference that each pirate transaction represents a lost legitimate sale. This is obviously overly simplistic: people buy pirated music, or make their own copies, because doing so is cheaper than buying the real thing from a retailer. It's not at all obvious that if the pirated version were not available then all those people would head straight for the nearest Musica. That said, it's pretty obvious that full-blown music counterfeiting is both illegal and unethical, and we ought not to support this industry by buying cheap counterfeits at flea markets and street traders. Your query, however, is about home-made pirate recordings*

*Many people who make pirate copies of CD's, particularly the 'home pirates' who don't actually make money out of piracy, think of themselves as modern day Robin Hoods - stealing from the obscenely rich recording company fat cats and their seriously overpaid 'artists', and giving to the poor (er, themselves). RIAA tries to undermine that kind of thinking by claiming that it's the consumer who is the 'ultimate victim' of piracy. Why? Because the poor consumer who buys a* *pirated copy is thereby denied the superior sound quality and flash packaging that comes with the real thing. Ag Shame.*

*While RIAA's argument is not particularly convincing, it's not clear that the Robin Hood argument holds water either. Presumably the idea is that in this sort of case stealing is justified by the nastiness of the person or persons being stolen from, and the real need of the person or persons the stealing is supposed to benefit. But does this really hold in this case?*

*While it's hard to feel too sorry for either Sony or their latest boy-band, we do need to ask ourselves whether they're really doing something wicked by making money out of their product. Perhaps the argument is that CD's are overpriced. Well, in a free market system there's a pretty good way of driving some product's price down - don't buy it.*

*If enough people agree with you, then the product won't sell and price will eventually come down. If it doesn't, then you were probably wrong about the overpricing in the first place. And let's face it, it's not as if music is such a fundamental need that you might die while waiting for the market to make things right. If you're really desperate, there's always the radio.*

*There are those who believe that there is price fixing going on in the music industry, and that piracy is a legitimate form of protest against the music barons. But if protest is really your goal, rather than just a convenient excuse for stealing, then copying your buddy's new CD is not a particularly effective way of doing it. Protests need to attract attention.*

*If you REALLY want to protest, and don't like any of the wide range of legal means of protesting that there are out there, then one good route would be to start openly selling counterfeit CD's outside your nearest big-name-brand record store, and wait to get arrested. You'll then get more than enough opportunity to get your message out through the media.*

*If protest is not really what's on your agenda, what should you do about the situation you describe? If you do really like the CD, buy yourself a legit copy and toss away the pirated version. If your buddy is concerned about why you didn't keep the pirated CD, you can always try RIAA's 'ultimate victim' line. And if you decide not to buy the CD, then get rid of the pirated version anyway, and go out and buy two copies of the latest release from your favourite South African artist or band - one for you and one for your friend.*

The next section is an insert on the operating software piracy in South Africa, but measured against the global amount in piracy.

**Industry toughens on piracy**

*HALF of the software in use in South Africa is illegal - that means it has not been paid for or is pirated. In the US 30% of software is pirated and in the UK, 35%. The rest of Africa has a software piracy rate into the 90% range.*

*The Business Software Alliance (BSA) - an anti-piracy umbrella body made up of large software companies - is getting tougher on offenders. Although in the past few months R300 000 has been recovered in out-of-court settlements, the BSA is in future going to prosecute offenders to the full extent of the law.*

*The latest world-wide software piracy figures released recently by the BSA show that South Africa is one of the few countries in the world that suffered from an increased rate of software piracy from 1997 to 1998.*

*Despite the decrease in the world-wide rate to 38% (from 40%), the amount of software pirated in South Africa rose to 49% (from 48%). This translates into a retail revenue loss to the local software industry of R580-million.*

*"The fact that the South African piracy rate increased is indicative of the extent of the local piracy problem," says Garry Hodgson, director of legalisation at Microsoft South Africa.*
*"For almost every copy of software sold, another is pirated or stolen. Theoretically, software resellers can get a rough indication of how much revenue they could gain through the eradication of software piracy by merely doubling their sales figures."*

*The illegal copying and distribution of software programs is the main obstacle to the growth of the software sector, which is reflected in revenue losses estimated at US11-billion to the worldwide industry in 1998.*

*This is just one of the findings published in the 1998 report on software piracy prepared by the International Planning Research Corporation (IPRC) for the BSA and Software and Information Industry Association (SAAI).*

*The IPRC report largely attributes the decreased rate of piracy world-wide to international economic recessions, particularly Asia, Eastern Europe and the Middle East. This suggests that* *the decline in piracy rates and dollar losses experienced in 1998 is not expected to continue into the future without increased enforcement of software copyright laws. "The increase in the local software piracy rate indicates that this is a crime that is not being taken seriously enough in South Africa," says Hodgson.*

*"Buying, selling or illegally copying software is supporting the South African crime problem and while Microsoft and the BSA will continue to raise public awareness about products that are legally protected by copyright, it is only through stricter legislation that this type of crime can be stopped. South Africans have to realise that software piracy is stealing - no more, no less - and criminals deserve to be punished."*

*As of July 1, 1999 the South African Government has six months to improve the local protection of intellectual property rights or face further unpleasantness from the Clinton administration's fair trade enforcers.*

*The US trade representative will be seeking assurances that government computers have been purged of unlicensed software and that SA will be in full compliance with the World Trade Organisation's trade-related intellectual property agreement (TRIPS) by January 1 next year.*

*The South African law does allow for some enforcement of copyright violation, and amendments to the copyright law in South Africa (the Intellectual Property Laws Amendment Act, effective October 1, 1997) have brought SA closer to compliance with its TRIPS obligations.*

*This is especially true in the scope of protection given to computer programs, protection of compilations of data and databases; and terms of protection for audio-visual works. However, even after these amendments, numerous areas of South Africa's enforcement practices fall short of full TRIPS compliance.*

**South Africa losing 30,000 jobs to piracy**

**By Tiisetso Motsoeneng, Daily Dispatch, 24 May 2006**

***About 36% of the software used by South African businesses is illegal, depriving more than 30,000 people of jobs in the multibillion rand information technology (IT) industry, say experts.***

*Although piracy rates among local businesses dropped 1% compared to last year, industry players said the numbers were still significantly high, representing at least R1,2bn in economic losses. "Software piracy remains one of the major hurdles to realising the potential of the information economy in South Africa, on the continent and around the world," said chairperson of the local arm of the Business Software Alliance (BSA) Stephan le Roux.*

*Le Roux was speaking on Tuesday at the release of a study commissioned by BSA, which found that some countries had piracy rates topping 90%, with Africa and the Middle East's gross domestic product losing about R10,3bn last year.*

*BSA is an industry body representing commercial software developers and their hardware partners. Its vice-chairperson Andrew Lindstrom said plenty of jobs could be created if the intellectual property protection laws were robustly enforced.*

*Besides software, South African intellectual property laws cover industries such as film, books and music.*
*The BSA study comes amid concerted effort from law enforcement officials to crackdown on DVD piracy, which crippled sales of the latest Leon Schuster movie Mama Jack and Oscar-winner Tsotsi.*

*A group of music heavyweights recently raided Johannesburg streets to wipe out pirated music CDs sold in some shops and by street vendors. BSA said that software piracy in the local industry has led to unfair competition, which has jeopardised foreign direct investment from international companies as there were low market returns.*
*Analysts said government needed to use all avenues to tackle the steep unemployment rate, which is sitting at 26,7%.*

*The report covering 97 countries pointed to a global software piracy rate of 35%, unchanged from last year's level. "This represents at least $34bn in economic losses worldwide - calculated according to the retail value of pirated software," BSA said.*

*The report also painted a gloomy picture of African countries' potential to implement successful intellectual property legislation, saying that software piracy on the continent averaged more than 70%.*

*Globally, piracy was most prevalent in Zimbabwe and Vietnam, which both showed rates of 90%.*
*"While we are upbeat that piracy levels are dropping, there is still a concern for our local economy that over a third of the software in use is illegal.*

*This concern rises when you look at some countries in Africa, where as few as one in ten copies of packaged software are legitimately paid for," said le Roux. He added that lowering software piracy would take constant work and investment but those investments could unlock benefits for the industry and local economies.*

*BSA said that if the global piracy rate were to drop 10% to 25%, about 2,4 million new jobs would be created, and a further $67bn in tax revenues would be added worldwide.*

**Bidorbuy Press Release - 13 September 2015**

**Bidorbuy declares war against piracy in South Africa!**

Bidorbuy, one of South Africa's largest online marketplaces, has taken a proactive stance against the selling of pirated goods online. Although e-commerce has shown tremendous growth over the past few years, its uptake has been hindered by various factors, one being consumers' concerns regarding pirated or illicit goods being sold online.

Looking at the number of people going online each year, the Internet has turned into a serious business medium, as the 25 000 people with dial-up Internet access in 1994 turned into an overall market of more than 5 million users in 2014. "

With the rapid growth and uptake of this medium locally, protection of intellectual property on the Internet has become an increasingly urgent issue", says Andy Higgins, managing director at bidorbuy. "Due to the difficulty controlling this aspect, more dealers of pirated or illicit goods will switch to the Internet to promote and sell their goods."

"Many people do not realise the high stakes involved, as failure to enforce piracy regulations in cyberspace could have repercussions for the economy as a whole," says Higgins. "Piracy is nothing less than serious theft. It is a crime that impacts right across our society, from government to the retail sector and right down to the individual customer, who, in buying pirated goods, end up with inferior products. The only winners are the criminals - something that needs to be stopped immediately!"

bidorbuy has acknowledged combating piracy as a top priority. Although the company is not experts in identifying pirated goods, it is working closely with industry bodies and authorities to ensure the problem of pirated goods on the www.bidorbuy.co.za site is combated effectively. Such bodies include the South African Police Services (SAPS), the Southern African Federation against Copyright Theft (SAFACT), the Business Software Alliance (BSA) and the Independent Communications Authority of South Africa (ICASA).

SAFACT, a trade association representing the entertainment industry, recently entered into an agreement with bidorbuy in the fight against the sale of pirated DVD movies and games online. "When considering the fact that the film industry loses approximately R200 million per annum through piracy, the agreement with bidorbuy is an important step forward in our continuous fight against this crime," says Fred Potgieter, general manager at SAFACT. "

Therefore we salute bidorbuy for this initiative and encourage other online auction sites to take similar responsibility to monitor what is being offered for sale on its site. This is of particular importance when we consider the increasing growth of Internet users in South Africa, many of which unfortunately use the Internet as a conduit for the sale of pirated films.

In the USA and Europe for example, the greatest threat to the software industry is the Internet and as such we should prepare for this trend locally."

The issue of software piracy and the resale of counterfeit goods have far-reaching implications - not only for the manufacturers of the products but for the economies of the countries in which the practice proliferates. IDC, the international research house, released the results of its software piracy study earlier this year after surveying 87 countries worldwide.

"South Africa's piracy rate stands at 37 percent - up one percent from last year and close to the global average of 35 percent. The general African average is a staggering 80 percent, with countries such as Zimbabwe topping 90 percent. This translates into Africa's economy suffering to the tune of $1bn per year. EMEA loses around $15bn. Globally, piracy costs approximately $33bn," explains Stephan Le Roux, chairman of the BSA in South Africa.

"Piracy remains a serious problem in South Africa and we are dedicated to play a role in the ongoing war that is being waged against the illegal importation and selling of counterfeit and pirated goods in the country. As such, we are keeping with our commitment to making the online marketplace a safe and secure place to conduct business," concludes Higgins.

### Professionalism in Computer Science

The surge of the computing industry has driven the growth of business and worldwide economies, revolutionising the way that information is generated and processed. It is therefore not hard to understand the importance of computers in modern society and business.

Although most of the world's population, and certainly business society, are capable of using computers to effective means, it is those that would consider themselves computing professionals that drive this industry. This essay intends to explore the implications of professionalism in computing, by comparing the Computer Society of South Africa (CSSA) with the British Computing Society (BCS), and consider the future role of professional computing societies.

### Characteristics of a profession

In order to understand computing as a profession it is necessary to understand professionalism as a whole and how computing fits into such a model. Society has put together a model, based around five characteristics, defining the roles and duties of a professional.

At the heart of any stream of expertise is a base knowledge common to all those practising in that expertise. In order to be considered a profession this base knowledge needs to be of an esoteric nature. This means that this knowledge must show deeper understanding of the expertise than that common to broader society. This understanding is usually the result or active research and experience.

A person acting as a professional should show signs autonomy in there work. Based on deeper understanding they should be capable of making appropriate decisions instead of following orders given by others. They should be able to regulate themselves and be able to set their own admission standards. A professional group should also have a standards of practice.

Such a professional society should have a formal organisation, responsible for the coordination of that society. This organisation must set standards for the professional society and regulate the skills needed by a person to become and remain a member of that society. The institution should be recognised by the country in which it is situated and have an authority amongst its members.

A code of ethics should be written and enforced by the professional body/organisation. This code of ethics serves the purpose or coordinating the society and maintaining autonomy. This code of ethics should govern the members of the professional society under any context they might find themselves whiles practising their profession.

Finally a profession should have a social function and benefit society in a unique way. The profession should add something to the worth of general society.

**Computing as a profession**

Computing makes for an interesting profession due to a number of features of the technology. The speed at which new technologies, in the computing world, are produced means that the base knowledge changes often and quickly, making it hard to coordinate such a society.

The technologies are also very new to society meaning that legislations and concepts often need to change to accommodate such a profession. This is why some people don't consider computing to be a valid profession.

The computing society meets almost all of the required characteristics of a profession but falls down at autonomy and social function. For example, one does not have to be a professional in order to be selected for certain jobs in the computing settings. Additionally computing fulfils a number of social functions but is not one in itself.

**Computer Society of South Africa (CSSA)**

The CSSA is the South African organisation heading up professional computing in South Africa. This organisation, much like computing in South Africa, is relatively young in comparison to other organisations in other areas of the world. Although the practices can be built upon those existing in other countries, the code of practices is still adjusting to the South African context.

As part of the attempt to coordinate the society the CSSA defines a code of practice in which it attempts to define the most professional and ethical way of acting in a business or academic setting. It defines a number of personal requirements such as keeping oneself, and their subordinates, up to date in the field of computing practices and legal requirements. Other personal requirements are focused on ensuring equal opportunities and accomplishing work ethically and efficiently.

It also defines a number of organisational and management requirements which is more concerned with broad principles. These requirements focus on communication, planning and delegation. Thirdly it focuses on contracting and the legal issues related to the drawing up of a contract and similar tasks.

It looks at privacy, security and integrity which are key to profession of computing, in relation to data management. These requirements are focused around the outlines of the privacy act of 1988. It looks at the requirements for developing new software and computing systems.

The aim of these requirements are to ensure that quality systems are developed and that in doing so all parties involved benefit as much as possible from the exercise. Similarly implementation is covered in a similar manner. Finally the issues concerning a system after it has been implemented and has gone 'live', and therefore the maintenance of the system.

**British Computing Society (BCS)**

In much the same way as the CSSA, the BCS also defines a code of practice and set of work ethics. The code of practice organises all practices into four different categories, general, key IT practices, education and research and business functions.

General practices defines ideas related to all aspects of professional computing, such as keeping up to date and technically competent. These practices refer to core ideas common to all professionals, such as adhering to regulations and using appropriate tools for given tasks.

The next batch of regulations are much more focused on computing as a profession. These regulations include project management, relationship management, security and many other related ideas all applied to the computing profession.

The practices related to education and research arch back to the core functions of a professional society. It focuses on shaping the base knowledge of the society and ensuring the best practices are encouraged in that society. One of the roles of a professional society is to shape the educational institutions, such as universities, that educate on their topic.

Finally, the last topic considered by the BCS, is focused on the business of computing. This focuses on the development life cycle of software development, documentation of systems, training, systems maintenance and many other similar tasks.

**Comparison**

Both the CSSA and BCS strive to accomplish the same targets in heading up the computer society for their respective countries. As a result they define very similar codes of operations and ethics. This demonstrates the international element of computing professionals. Through the use of the Internet, developers create products for the international market instead of just limiting themselves to their local market place. It is therefore understandable that computing professionals around the world share similar mind sets and objectives.

However one of the main differences between the CSSA and the BCS is the time that these organisations have been operational. The BCS has been around since the invent of the computer industry, whereas the CSSA is a much more recent development. As such the BCS has a very traditionalists approach to computing professionalism.

The British professional society is more focused on innovation and the research sides of computing society. The CSSA is a more modern approach to computing professionalism. It focuses more on the implementation and practical side of the industry. The shorter life span of the CSSA is also apparent in their code of practice in that it is not as refined or adapted to greater society as the BCS.

Differences are also noticed when considering the difference social settings in which the two institutions find themselves. The South African setting is a much poorer economy and as such the professional institution are more focused on making the market place grow in South Africa. The ethics behind the code of operations is also more focused on equal opportunities which, again, stems from the South African setting.

**Future of CSSA**

As stated before the CSSA is much younger in comparison to the BCS and as such the future of the CSSA is of much interest. It would make sense that the BCS is a decent approximation to the future of the CSSA but in my own opinion the future of the CSSA is much more dependant on the economic future of South Africa. The CSSA encourages the development of the local economy rather than that of the international economy and as such plays an important role in developing the computing industry in South Africa.

Currently, as the CSSA is still relatively new, the institution is still gaining support and therefore authority over the industry. However as they gain more support they are likely to play an important role in the development of the computing industry in South Africa.

**Ethics and Professionalism**

There are several ways of identifying and deciding ethical issues. One of the most common ways of categorizing these approaches is the rules vs. consequences criteria. The first argues that our actions should be guided by general rules or principles: do not harm; tell the truth; do not steal; respect for persons.

The second argues that we should assess the “rightness” of an action or decision by the consequences that will likely result. Most commonly the second approach identifies some “value” or values, and measures the actions by the extent to which these values are or are not enhanced, or progress made toward certain goals, such as a better life for all.

On reflection is should be clear that there is no consensus about which of these is the more appropriate. The foundation of all security systems is formed by moral principles and practices of those people involved and the stan-dards of the profession. That is, while people are part of the solution, they are also most the problem. Security problems with which an organization may have to deal include: responsible decision making, confidentiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage. It is easy to sensationalize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

**A. Ethics**

**1. Ethics and Responsible Decision-Making**

The foundation of all security systems is formed by moral principles and practices of those people involved and the standards of the profession. That is, while people are part of the solution, they are also most the problem. Security problems with which an organization may have to deal include: responsible decision making, confiden-tiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage. It is easy to sensational-ize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

**2. Confidentiality & Privacy**

Computers can be used symbolically to intimidate, deceive or defraud victims. Attorneys, government agencies and businesses increasingly use mounds of computer generated data quite legally to confound their audiences. Criminals also find useful phony invoices, bills and checks generated by the computer. The computer lends an ideal cloak for carrying out criminal acts by imparting a clean quality to the crime.

The computer has made the invasion of our privacy a great deal easier and potentially more dangerous than before the advent of the computer. A wide range of data are collected and stored in computerized files related to individuals.

These files hold banking information, credit information, organizational fund raising, opinion polls, shop at home services, driver license data, arrest records and medical records. The potential threats to privacy include the improper commercial use of computerized data, breaches of confidentiality by releasing confidential data to third parties, and the release of records to governmental agencies for investigative purposes.

### 3. Piracy

Microcomputer software presents a particular problem since many individuals are involved in the use of this software. Section 117 of the copyright laws, specifically the 1980 amendment, deals with a law that addresses the problem of backup copies of software. This section states that users have the right to create backup copies of their software.

That is, users may legally create a backup copy of software if it is to be held in archive. Many software companies provide a free backup copy to users that precludes the need for to users purchase software intended to defeat copy protection systems and subsequently create copies of their software.

If the software purchased is actually leased, you may in fact not even be able to make backup copies of the software. The distinc-tion between leasing and buying is contained within the software documentation. The copyright statement is also contained in the software documentation. The copyright laws regarding leased material state that the leasor may say what the leaseholder can and cannot do with the software. So it is entirely up to the owner of the soft-ware as to whether or not users may make backup copies of the software.

The software industry is prepared to do battle against software piracy. The courts are dealing with an increasing number of lawsuits concerning the protection of software. Large software publishers have established the Software Protection Fund to promote anti-piracy sentiment and to de-velop additional protection devices.

### 4. Fraud & Misuse

The computer can create a unique environment in which unauthorized activities can occur. Crimes in this cate-gory have many traditional names including theft, fraud, embezzlement, extortion, etc. Computer related fraud includes the introduction of fraudulent records into a computer system, theft of money by electronic means, theft of financial instruments, theft of services, and theft of valuable data.

### 5. Liability

Under the UCC, an express warranty is an affirmation or promise of product quality to the buyer and becomes a part of the basis of the bargain. Promises and affirmations made by the software developer to the user about the nature and quality of the program can also be classified as an express warranty.

Programmers or retailers possess the right to define express warranties. Thus, they have to be realistic when they state any claims and predictions about the capabilities, quality and nature of their software or hardware. They should consider the legal aspects of their affirmative promises, their product demonstrations, and their product description.

Every word they say may be as legally effective as though stated in writing. Thus, to protect against liability, all agreements should be in writing. A disclaimer of express warranties can free a supplier from being held responsible for any informal, hy-pothetical statements or predictions made during the negotiation stages.

Implied warranties are also defined by the UCC. These are warranties that are provided automatically in every sale. These warranties need not be in writing nor do they need to be verbally stated. They insure that good title will pass to the buyer, that the product is fit for the purpose sold, and that it is fit for the ordinary purposes for which similar goods are used (merchantability)..

### 6. Patents and Copyright Law

A patent can protect the unique and secret aspect of an idea. It is very difficult to obtain a patent compared to a copyright (please see discussion below). With computer software, complete disclosure is required; the patent holder must disclose the complete details of a program to allow a skilled programmer to build the program.

Copyright law provides a very significant legal tool for use in protecting computer software, both before a secu-rity breach and certainly after a security breach. This type of breach could deal with misappropriation of data, computer programs, documentation, or similar material. For this reason the information security specialist will want to be familiar with basic concepts of copyright law.

The United States, United Kingdom, Australia, and many other countries have now amended or revised their copyright legislation to provide explicit copyright laws to protect computer program. Copyright law in the United States is governed by the Copyright Act of 1976 that pre-empted the field from the states. Formerly, the United States had a dual state and Federal system. In other countries, such as Canada, the courts have held that the un-revised Copyright Act is broad enough to protect computer programs. In many of these countries the re-form of copyright law is actively underway.

### 7. Trade Secrets

A trade secret protects something of value and usefulness. This law protects the unique and secret aspects of ideas, known only to the discoverer or his confidants. Once disclosed the trade secret is lost as such and can only be protected under one of the following laws.

The application of trade secret law is very important in the computer field, where even a slight head start in the development of software or hardware can provide a signifi-cant competitive advantage.

### 8. Sabotage

The computer can be the object of attack in computer crimes such as the unauthorized use of computer facilities, alternation or destruction of information, data file sabotage and vandalism against a computer system. Computers have been shot, stabbed, short-circuited and bombed.

**Activities – In your groups**

Explain how the computer industry supports equality of opportunity

Explain how the computer industry is against computer software piracy

Identify ways in which piracy is addressed in South Africa

You are now ready to go through a check list. Be honest with yourself

Tick the box with either a √ or an X to indicate your response

□ I am able to describe professionalism for the computer industry in South Africa

□ I am able to describe the codes of practice for professionalism in the IT industry in South Africa

□ I am able to describe the code of ethics in the computer industry in South Africa

You must think about any point you could not tick. Write this down as a goal. Decide on a plan of action to achieve these goals. Regularly review these goals.

**My Goals and Planning:**

__________________________________________________________________

__________________________________________________________________

__________________________________________________________________

__________________________________________________________________

__________________________________________________________________

__________________________________________________________________